

eSENTIRE

The Hunt for VENOM SPIDER

PART 2

*Tracking the Real Mastermind Behind the Cyber Weapon of Choice
for Two of Russia's Most Notorious Internet Crime Gangs*

by Joe Stewart and Keegan Keplinger

Security Researchers with eSentire's Threat Response Unit (TRU)



eSENTIRE
Threat Response Unit

Executive Summary

For the past 21 months, eSentire's security research team, the Threat Response Unit (TRU), has been tracking, analyzing, and defending its customers from one of the most capable and stealthy malware suites—Golden Chickens. Golden Chickens is operated as a Malware-as-a-Service (MaaS), and it is the “cyber weapon of choice” for two of the longest-running and notorious financial crime groups: Russia-based FIN6 and Cobalt Group. The two criminal operations are estimated to have collectively caused financial losses over USD **\$1.4 Billion**.



Are Golden Chickens attacks still occurring? Is this MaaS still a threat?

According to eSentire, TRU saw cyberattacks using the Golden Chickens MaaS throughout 2022 and into January of 2023. During that time, TRU detected and shut down nine separate Golden Chickens incidents and there were two additional failed Golden Chickens attacks. The eleven companies targeted in these incidents represent e-commerce companies and service firms, and all of them have online payment systems. They include companies and organizations in the following industries: accounting, aviation parts sales, legal firms, workforce solutions, insurance, energy providers, food suppliers and building suppliers. Interestingly, during the first week of May 2023, TRU found that two identical samples of the Golden Chickens VenomLNK component were uploaded to VirusTotal. One sample was uploaded from the Ukraine, and one was uploaded from the U.S. This might indicate an attempt by threat actors to launch a new attack campaign or it might indicate testing by the threat actors.

Although in the past, the malware has primarily been used to steal credit cards, debit cards, and banking credentials, there is nothing to say that the Golden Chickens operator won't bring on a new customer, whose sole objective is to infect victims with ransomware. As we saw with the ransomware attack, which crippled the **UK's Royal Mail** service and the attack that hit Canada's Hospital for Sick Children, if a customer of Golden Chickens decides to use this malware primarily to spread ransomware or destructive malware, Golden Chickens will cause far much danger than the theft of payment cards and banking credentials.

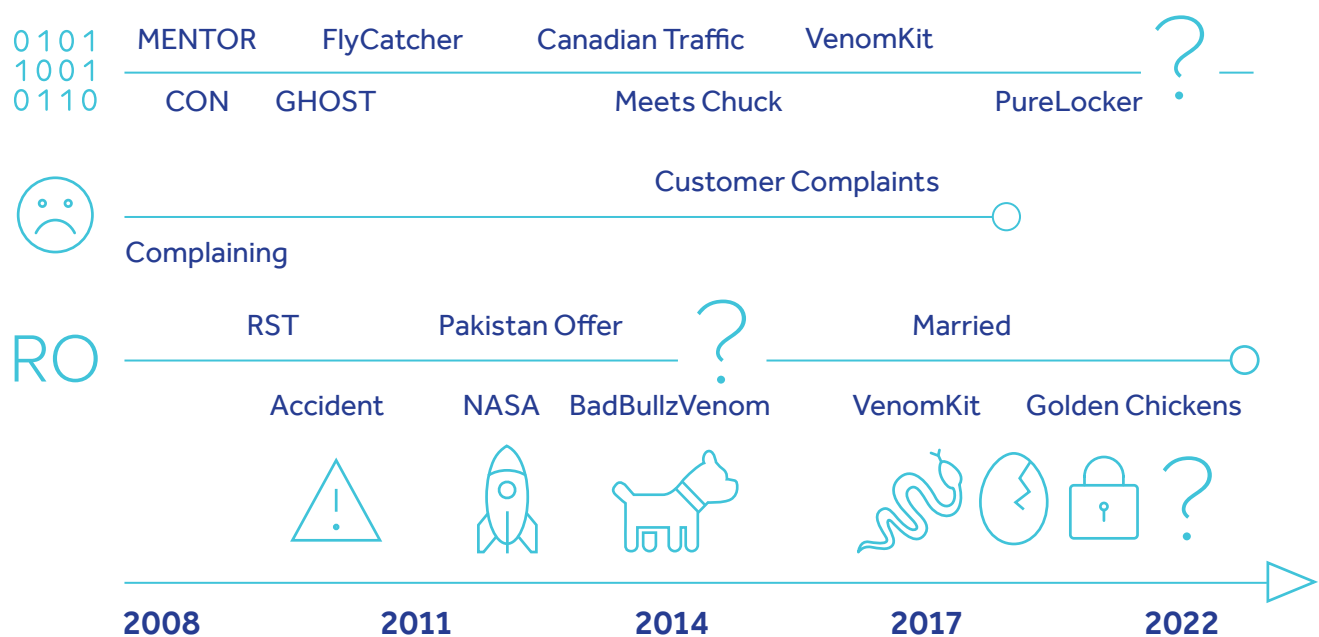
On August 11, 2022, TRU revealed in its security report: **Unmasking VENOM SPIDER – The Hacker Behind the Cyber Weapon of Choice for Two of Russia's Most Notorious Internet Crime Gangs** that it had discovered the identity of one of the threat actors behind Golden Chickens. The threat actor self-identifies as “Chuck from Montreal”. He operates an account on the Russian-language forum, Exploit.in, under the name “badbullzvenom” and is referred to as VENOM SPIDER by CrowdStrike researchers.

TRU also revealed in the report that “Chuck from Montreal” is just one of two criminals operating the badbullzvenom and badbullz accounts, leaving cyber experts wondering who is the other threat actor, using these accounts, and running the Golden Chickens MaaS? For five months, TRU sifted through hundreds of forum chats from different threat actors, some going back to 2008, so as to answer this question. TRU has found the answer. This new report, Part 2, tracks the identity of the true mastermind behind Golden Chickens, and it outlines, in meticulous detail, how his identity was discovered. eSentire is partnering with law enforcement based on the information gathered, thus we are not currently providing his aliases and the names of the various malware he has developed. As such, we have assigned Venom Spider the code name: “Jack.”

Key Findings:

- TRU discovered the second threat actor behind Golden Chickens self identifies as "Jack" and was born in a small Romanian town called Mizil
- TRU tracked "Jack's" Internet activities going back to 2008, when he was 15
- "Jack" seems to have picked up coding at an early age, although TRU could find no evidence of any formal education. Since age 15, "Jack" has displayed a strong interest in developing malware and tools to assist in cybercrime
- "Jack" has a short fuse. As early as 19, "Jack" had already gained a reputation as a "Ripper/Scammer"
- In July 2022, "Jack" has a \$200,000 bounty placed on his head, on Exploit.in, by a threat actor who accuses him of stealing \$1 million dollars from him
- Like "Chuck from Montreal", "Jack" uses multiple aliases on forums, social media, and Jabber accounts, and goes to great lengths to disguise himself

Threat Actor Career Timeline:



Conclusion

TRU has discovered “Jack’s” real name, as well as his wife, sisters, and mother. TRU has found pictures of him and his family members, the city in which he lives, where he likes to vacation, the business he purports to run, and that he and his wife enjoy traveling to the major cities in Europe.

TRU found that “Jack” is considered, by many of his customers, to be a “Scammer” so much so that in July 2022, a cybercriminal going by the alias “babay” went on a Russian forum, Exploit.in, and issued a bounty in the amount of \$200,000 for information leading to “Jack’s” real identity.

Like “Chuck from Montreal”, “Jack” uses multiple aliases for the underground forums, social media, and Jabber accounts, and he too has gone to great lengths to disguise himself. TRU also discovered that “Jack” has taken great pains to obfuscate the Golden Chickens malware, trying to make it undetectable by most AV companies, and strictly allowing only a small number of customers to buy access to the Golden Chickens MaaS. Also, his malware must only be used for targeted attacks.

Because of eSentire’s investigation, “Jack”, like “Chuck”, has lost his anonymity. TRU also continues to track any updates in the Golden Chickens source code and discover new Golden Chickens attack campaigns. TRU expects to see further targeted attacks, leveraging this malware, being launched against e-commerce companies and other organizations with payment systems in the foreseeable future.

It is rare to uncover this level of detail about two threat operators, and this report illustrates the breadth and expertise of eSentire’s Threat Response Unit. This intelligence, including many of the underground forum conversations “Jack” and “Chuck from Montreal” had with other threat actors, has been extremely valuable. It has helped TRU better decipher “Jack” and “Chuck from Montreal’s” Tactics, Techniques and Procedures (TTPs), as well as the actual origins of the Golden Chickens MaaS and its ongoing operations. With this knowledge, TRU continues to hone its defenses, protecting eSentire’s global customer base from well-orchestrated attacks utilizing the Golden Chickens MaaS.

TRU’s objective with this report is to share their research with other security teams so that they can better defend their critical data from attacks using the Golden Chickens malware suite. Also, with the real identity of the Golden Chickens author, law enforcement has an opportunity to make an arrest. This would interrupt the malware supply chain of top financial crime gangs, such as FIN6, Cobalt Group and others, and it would disrupt their business forcing them to find another malware source. The balance of this report includes:

- An overview of how TRU discovered the alias of the second threat actor behind the Golden Chickens MaaS.
- A detailed account of the investigation and subsequent identification of the real man who created and operates the Golden Chickens MaaS.
- A unique look into the making of a hacker. Readers will see how the creator of one of the most sophisticated suites of malware progresses from a young, naïve teenager, interested in computers and malicious software, to a young adult, writing password stealers and crypters, to a full-grown man who has created one of the most capable malware suites being used in cybercrime today. Readers will get a glimpse into the personal and business side of a longtime hacker.
- Insights and security recommendations from TRU.

Full Report

For the past 21 months, eSentire's security research team, the Threat Response Unit (TRU), has been tracking, analyzing, and defending its customers from one of the most capable and stealthy malware suites—Golden Chickens. Golden Chickens is operated as a Malware-as-a-Service (MaaS), and it is the “cyber weapon of choice” for two of the longest-running and notorious financial crime groups: Russia-based FIN6 and Cobalt Group (the two criminal operations are estimated to have collectively caused financial losses over USD \$1.4 Billion).

On August 11, 2022, TRU revealed in its security report: [Unmasking VENOM SPIDER – The Hacker Behind the Cyber Weapon of Choice for Two of Russia's Most Notorious Internet Crime Gangs](#) that it had discovered the real identity of one of the threat actors behind Golden Chickens. The threat actor self identifies as “Chuck from Montreal”. In fact, he does live in Montreal, Canada and operates various underground forum accounts, under the aliases badbullz and badbullzvenom. This includes one on the Russian-language forum, Exploit.in, under the name badbullzvenom. He is referred to by CrowdStrike researchers as [VENOM SPIDER](#).

TRU also revealed in the August report that “Chuck from Montreal” is just one of two cybercriminals operating the badbullzvenom and badbullz accounts. One of the clues that led TRU to that conclusion is that they discovered in forum chats, two random mentions of the badbullzvenom account being shared between two people (See Figures 1 and 2).

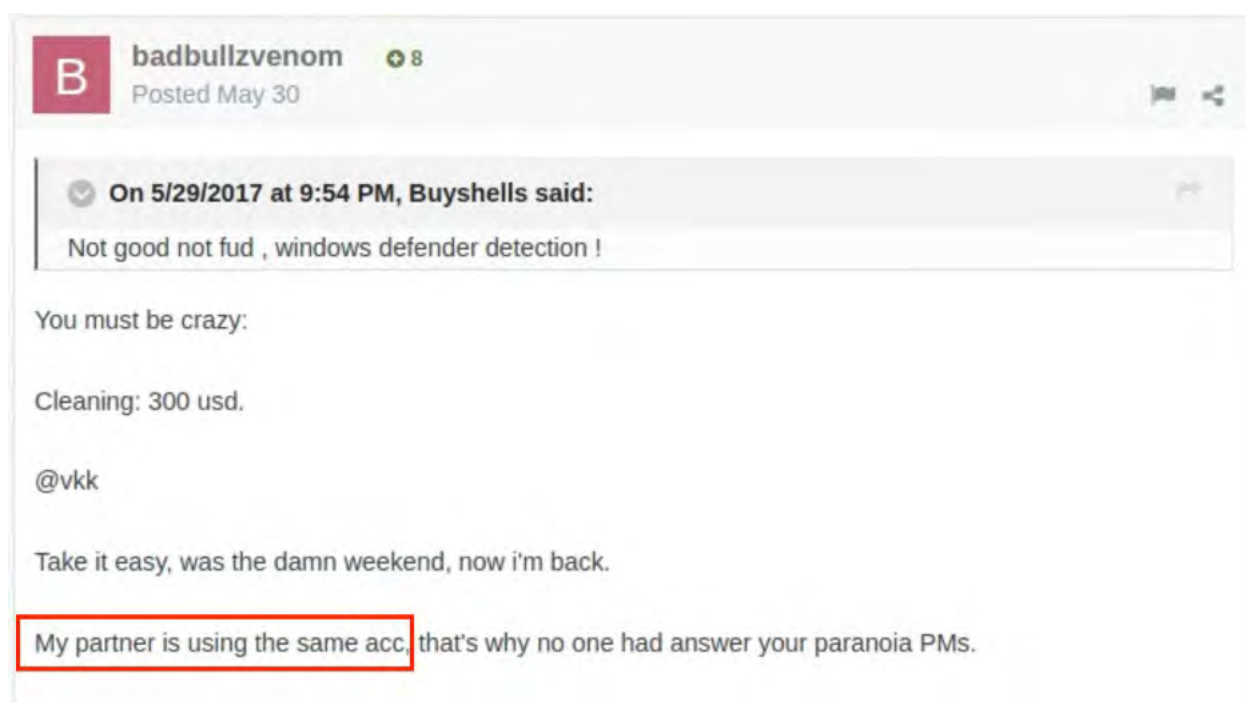


Figure 1—A dispute thread in Exploit.in.

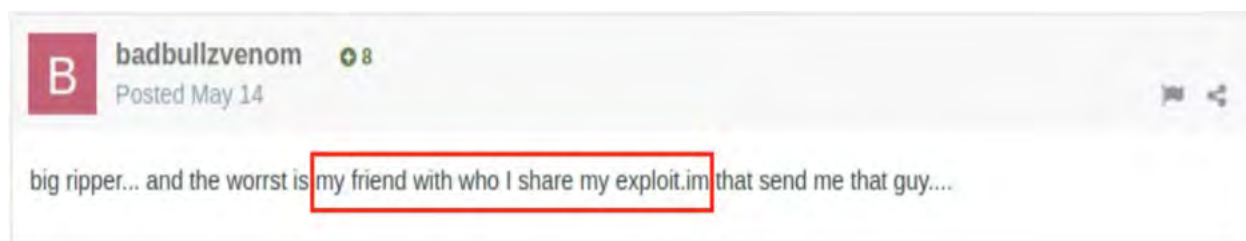


Figure 2—EA post from badbullzvenom in the forum, Exploit.in

It wasn't just the forum posts that made TRU skeptical about "Chuck from Montreal" being the actual developer of the Golden Chickens malware. Golden Chickens is a stealthy, highly functional suite of malicious software. In reviewing "Chuck from Montreal's" chats, it did not appear that he had the interest nor the skills to create this sophisticated malware. In TRU's opinion, he showed more interest in being a cash-out guy—a criminal that monetizes stolen credit cards, debit cards, bank account data, etc.

Thus, **remained the questions**: who is the second threat actor operating the badbullzvenom account, and what part does he play in the Golden Chickens MaaS? TRU set out to find these answers. For the past five months, two researchers with TRU: Joe Stewart and Keegan Keplinger have sifted through hundreds of chats, many from leaked forum databases, so as to answer this question. Not only did they discover the identity of the second threat actor, they also found which city he is currently living, the name of his wife, the business he purports to run, various vacations he has taken, and that he self identifies as "Jack."

TRU has been able to build a picture of "Jack's" progression from a young, naïve teenager, interested in computers and malicious software, to a young adult, writing password stealers and crypters, to a full-grown man who has created one of the most capable malware suites being used in cybercrime today.

"Jack" starts out as a teenager by writing simple software code. As his skills improved, he began building simple password stealers. TRU then sees him progress to the point where he can make crypters (software that is used to encrypt, obfuscate, and manipulate malware, so it can slip by anti-virus and anti-malware undetected). Moving on from making crypters, TRU saw him create a malicious document builder. "Jack" used his past knowledge to slowly add more malware modules to his malicious document builder, such as a JavaScript backdoor and a password stealer. He finally puts all of his knowledge together, and his Golden Chickens MaaS comes out in 2017.

All roads lead to Jack

When first tracking "Jack," TRU had only one lead to go on in their quest to discover the identity of the second threat actor behind badbullzvenom. Sifting through every underground chat TRU could find from badbullz and badbullzvenom, they finally came across a 2013 post in the forum Lampeduza, where badbullz was trying to sell credentials for a Canadian bank-issued credit card that had a balance of \$13,000. To contact him privately, badbullz provided a jabber account TRU had not seen previously: maratbalagula@zloy.im (Figure 3).

Note: eSentire is partnering with law enforcement, based on the information gathered, and as such we are not currently providing the jabber accounts or "Jack's" aliases, email addresses, and the names of the various malware "Jack" has developed. TRU is substituting "Jack's" aliases for the code word LUCKY.

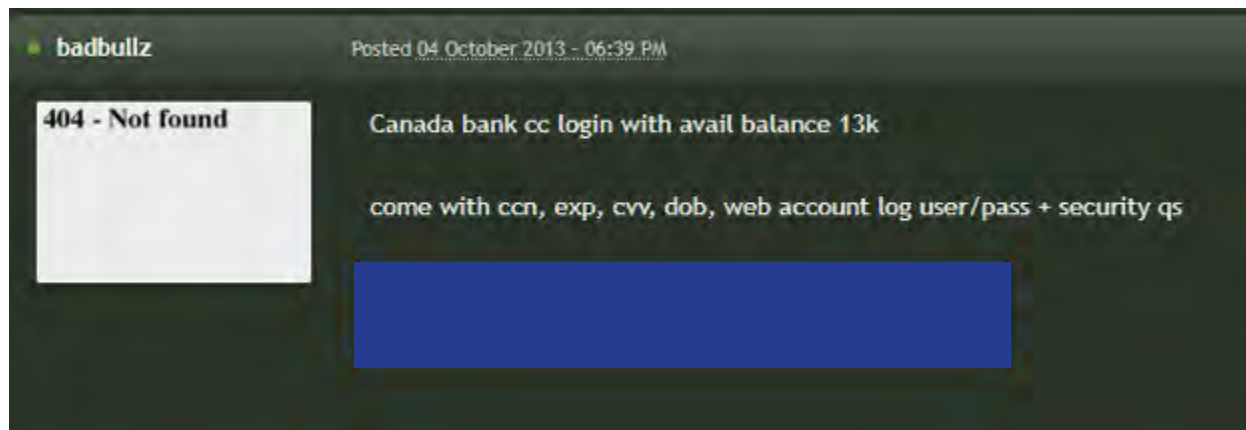


Figure 3—A 2013 post in Lampeduza forum where badbullz is trying to sell stolen credentials for a credit card account, issued by a Canadian bank, with a \$13,000 available balance. Badbullz provides a jabber i.d. TRU had never seen before.

With this small lead, TRU began combing through hundreds of chats on underground forums, looking for that unique jabber account. They finally came upon a thread in the popular Russian hacker forum, Verified, where a threat actor going by the alias LUCKY, used the Jabber address (See Figures 4 and 5).

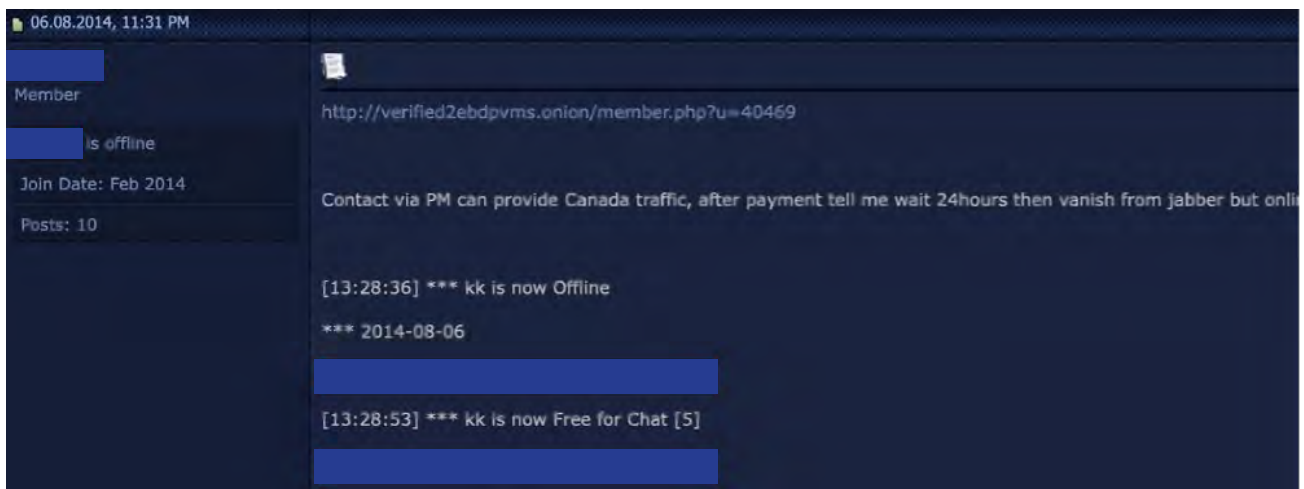


Figure 4—A chat on Verified, a popular Russian hacker forum, where threat actor LUCKY uses the same jabber account as badbullzvenom.



Figure 5—The continuation of a chat on Verified, a popular Russian hacker forum, where threat actor LUCKY uses the same jabber account as badbullzvenom

Who is LUCKY and how is he connected to “Chuck from Montreal?” and the Golden Chickens MaaS?

The first question TRU asked themselves is “Who is this LUCKY and how is he connected with ‘Chuck from Montreal?’” It was the seemingly insignificant discovery of an account going by the alias, LUCKY, that was to break the investigation wide open.

Tracking LUCKY

With this clue, TRU immediately began combing the hacker forums for any chats attributed to LUCKY. The first forum posts TRU found were from 2008, when LUCKY was 15 years old. TRU was able to learn LUCKY's date of birth because he entered it into various forums when registering to become a member. He also revealed his age in some of the chats and the date matches what he entered into the forums. One of these forums was the Romanian Security Team (RST), and it was in the RST forum that TRU also found that LUCKY used two additional aliases: best_LUCKY and B3st. The RST has a large following from residents of Romania who are interested in cybersecurity. The forum includes white hats and black hats. LUCKY's posts in the forum portray him as a novice. However, from the chats, one can tell that he is very interested in learning how malware works, and he is intent on trying to establish a reputation for himself. (See Figure 6).

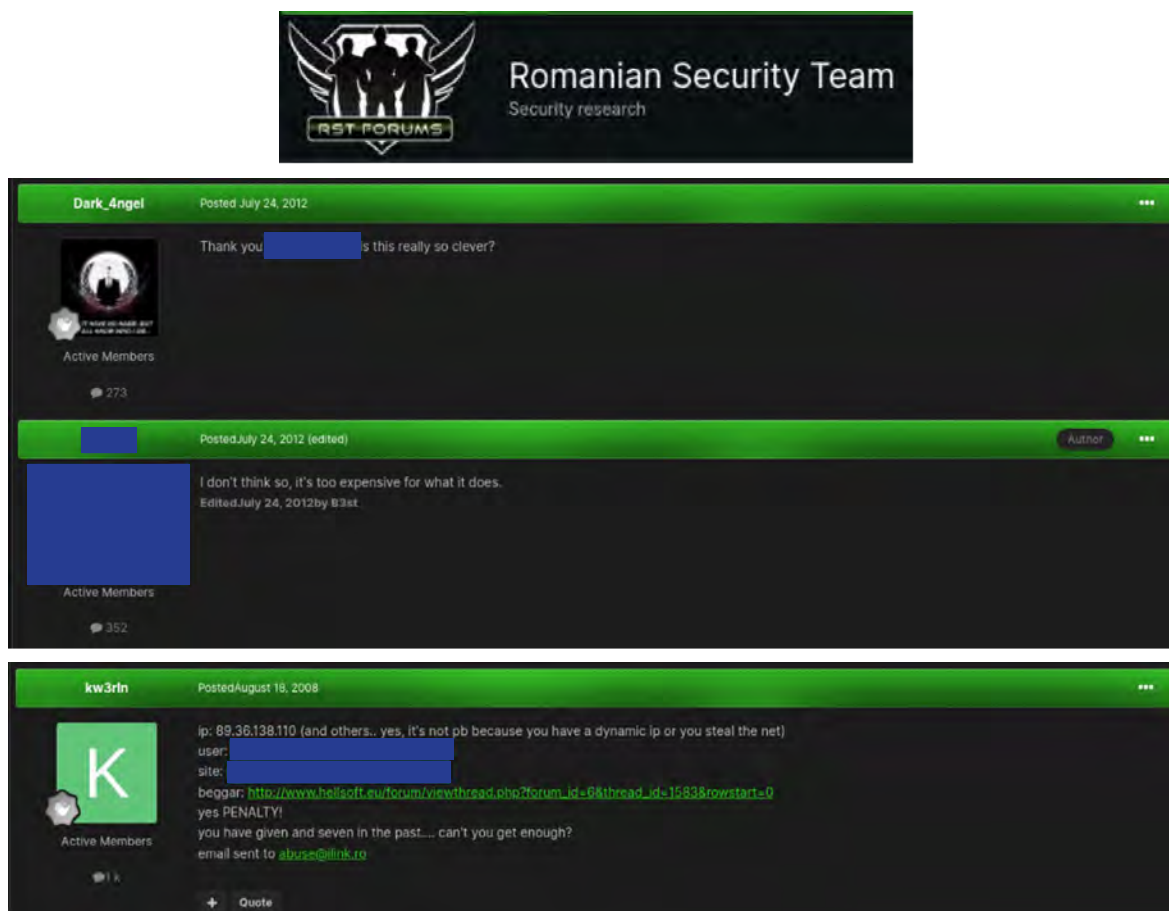


Figure 6—References to LUCKY using two similar aliases.



Sometime between 2007 and 2008, LUCKY released a new malware tool. We have given it the codename Voyer. It is designed to steal a victim's Yahoo instant messages, which technically is not difficult if you already have access to the victim's PC. However, in late 2008 and early 2009, LUCKY's technical skills appear to be improving. He comes out with another malware tool. It can intercept, and record keystrokes entered by the victim into any desktop window, as well as send messages to the victim, via popup dialogs. TRU has given it the codename FlyCatcher. Additionally, it can perform some rudimentary actions to control the system such as logging out, rebooting, and shutting down (See Figure 7)

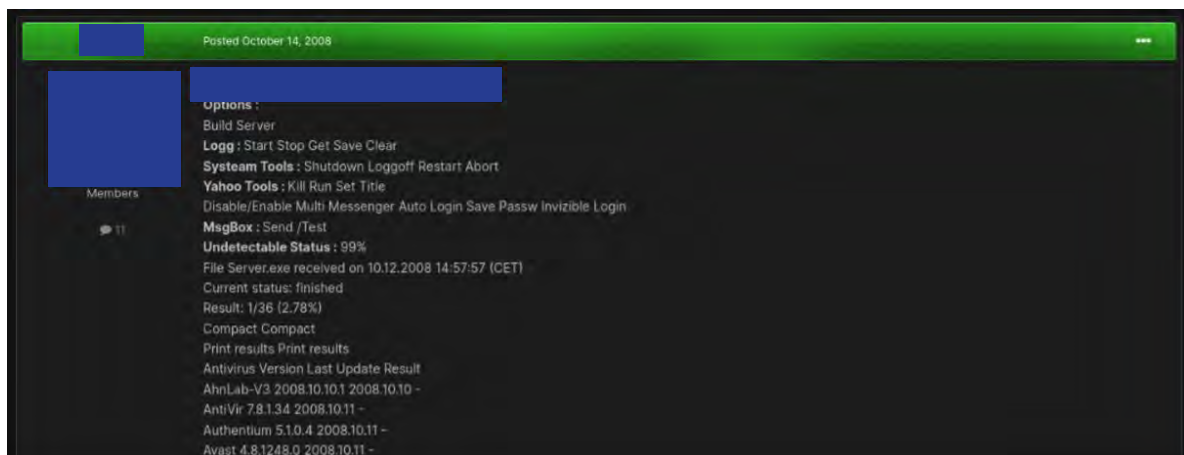


Figure 7—LUCKY promoting FlyCatcher on an underground forum, listing its various functionality.

LUCKY seems to have picked up coding at an early age, although TRU could not find any evidence that LUCKY had any formal education, and in fact, he said in one chat that he got out of school as soon as he could, making the comment "I only go to school to drink my coffee." Between 2009 and 2010, LUCKY proceeded to publish a new password stealer that TRU is calling CON. LUCKY dedicated CON to an underground forum for which he was a member. It appeared that LUCKY was paying homage to the forum, not only because he named his password stealer after it, but in a 2012 post, where he is promoting the stealer's many attributes, he states it is: "produced for the forum".

LUCKY does not seem to charge for the password stealer and according to the 2012 post, CON is capable of stealing website credentials saved in different web browsers, including Internet Explorer, Google Chrome, Mozilla Firefox, etc. LUCKY also claims the tool can steal messages and stored credentials from MSN Messenger and Yahoo Messenger, as well as credentials for VPN and FTP applications installed on the victim's computer (See Figure 8).

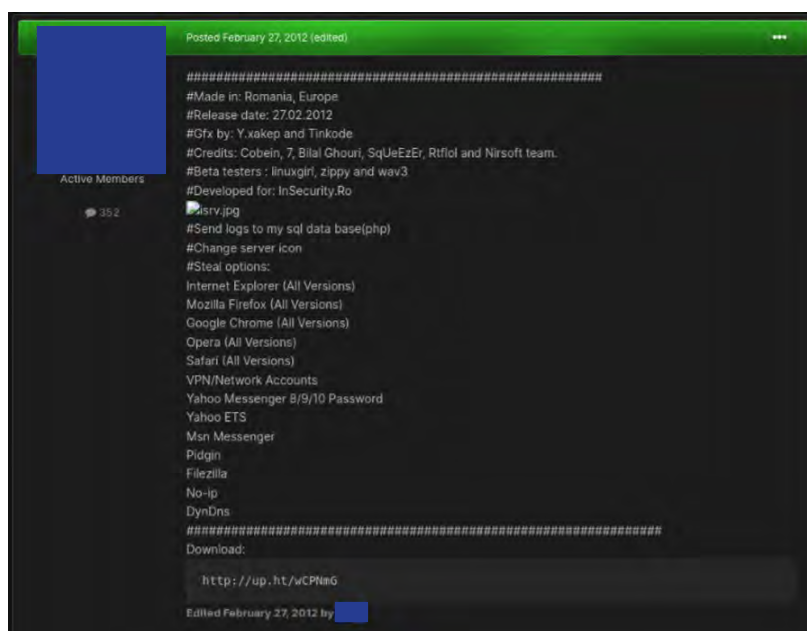


Figure 8—A 2012 underground forum post in which LUCKY describes the functionality of the tool, CON. . He first released CON sometime between 2009 and 2010.

Young LUCKY begins upping his cyber skills

By the second half of 2009, LUCKY started upping his game. He released a crypter TRU has given the codename GHOST. A crypter is a type of software that can encrypt, obfuscate, and manipulate malware to make it harder for security programs to detect the malware. Various forum posts reveal that LUCKY's encryption tool was well received by the hacker community, spurring him on to add new enhancements.

One can also begin to get a sense of LUCKY's personality, and that he has a sarcastic streak, demonstrated in the screenshot where he is advertising his new crypter he states: "First of all, this crypter is the worst, please don't buy it!" (See Figure 9).

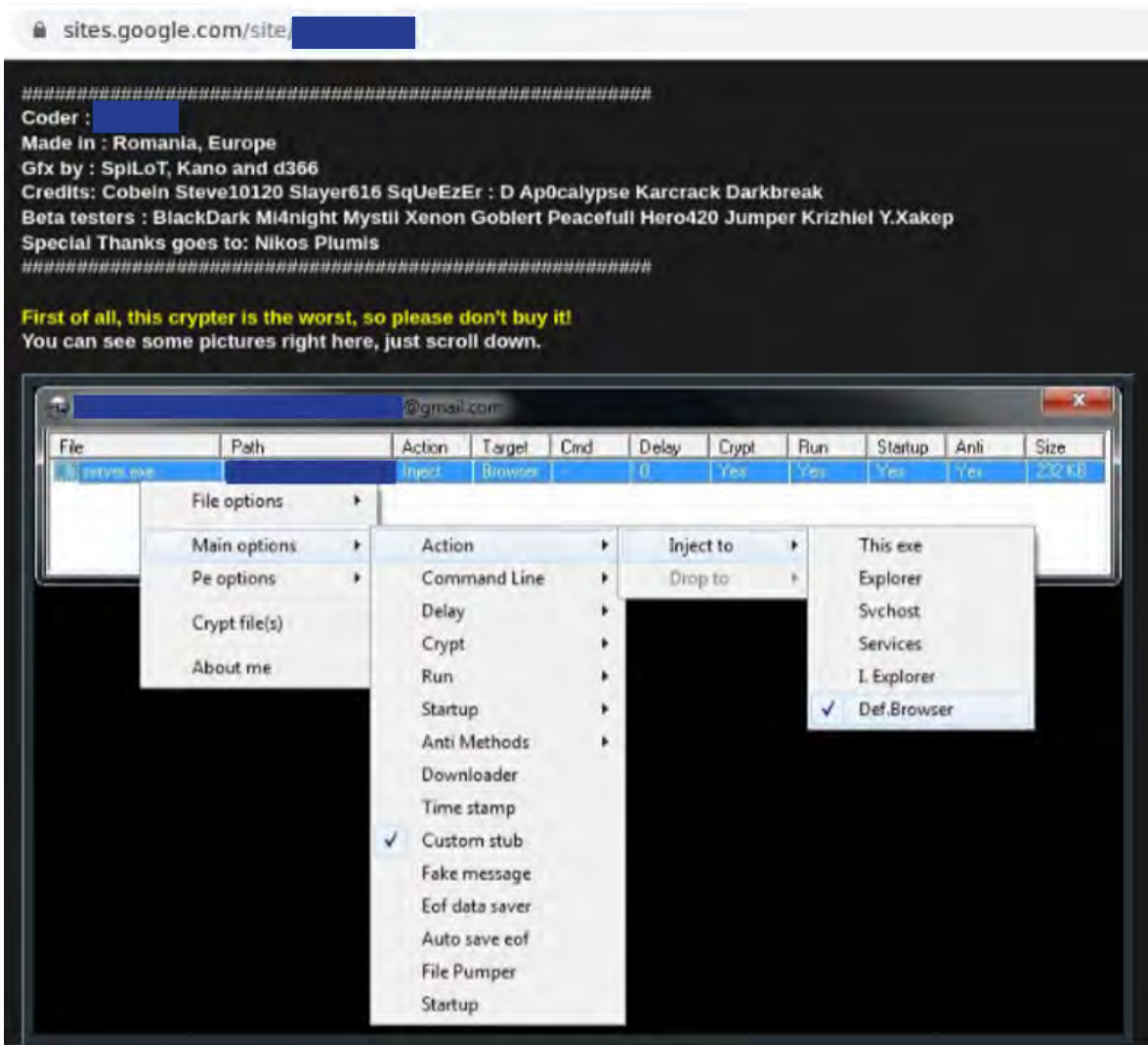


Figure 9—LUCKY established a website for his new crypter, GHOST, where he lists the crypter's functionality, and he gives credit to fellow threat actors who have assisted him in its development and testing of the crypter.

LUCKY suffers a heartbreaking loss

In 2010, when LUCKY was just 17, he suffered a heartbreaking loss. He wrote an email to his customers telling them that, for the time being, he was ceasing development on GHOST because he was having a lot of trouble. LUCKY said, "I got many personal and financial problems in last month, like my father died about two weeks ago in one car accident, before 2 days i haved (sic) one car accident with no victims...and so on. Since then I lost my motivation..."

LUCKY went on to say in the email, "Everyone who will pay 15 usd will get next crypter for free, it will be named > MENTOR(really). MENTOR will be dedicated to my father, maybe sounds crazy for you...but this is it. And last, sorry for all the problems I've caused to you because I didn't updated (GHOST)." See Figure 10.

```
text 0.87 KB | None
1. Hi,
2.
3. I don't really know how to start this mail, but here we go.
4. I got many personal and financial problems in last month, like my father died about two weeks ago in one car accident, before 2 days
   i haved one car accident with no victims .. and so on.
5. Since then i lost my motivation, i wish i never talk with you in this situation.
6.
7. For get new updates all customers need to pay 15 usd at my liberty reserve account, excluding new customers(2-3 week recent
   customers).
8. I will work hard at FC, like before, if i can't keep it up, i will sell the source and start new project.
9. Everyone who will pay 15 usd will get next crypter for free, it will be nammed > [redacted] (really).
10. [redacted] will be dedicated to my father, maybe sounds crazy for you .. but this is it.
11. And last, sorry for all the problems i've caused to you because i didn't updated [redacted]
12.
13. Best Regards,
14. [redacted]
```

Figure 10—The email LUCKY sends to his GHOST customers explaining that he has not made any new updates to GHOST recently because he was experiencing many problems, including the sudden death of his father.

Don't bite the hand that feeds you

After LUCKY's 2010 email alerting his customers about his father's death, TRU saw nominal communications from LUCKY or about LUCKY until a post from a disgruntled client dated May 6, 2012. The client went by the alias "parkingcash." Parkingcash said he had purchased the GHOST software in July 2011, and that LUCKY advertised three months of customer support with the purchase. However, according to parkingcash, LUCKY ignored his repeated requests for help.

Upset, parkingcash posted his complaint about LUCKY on an underground forum called Open SC warning other potential buyers: "He never reply to me in three months...That is the way of how this sh__ treat with his client. It happened a few months ago but I decided to post it here to make sure more people can see it, and do not buy anything from him, if you don't want to be treated like this." Parkingcash even went as far as to include screenshots of the chats between he and LUCKY in the complaint (See Figure 11).

06-05-2012 #1

parkingcash • Member

Join Date: Dec 2010
Posts: 88

Scam of [redacted], How he treats his client.

Story:

I Bought [redacted] crypter on July of 2011, Paid him 75 USD by LR. everybody knows [redacted] said he offers 3 month updates support, and this is also what he wrote on his site. But after i bought it, i only got the update once from his Email(its in the same week after bought the crypter), and after it , never receive new update again, although his USG is detected by 98% of AVs.

and on the August of 2011, i tried to contact him to ask what happend. i contacted him serveral times , he ignored me on msn even he is online, and i emailed him 4 times at least in 3 month(emailled him to both of his emails, 100% no mistake), but he never reply me....

But on Dec of 2011, I got an email from him , he is promoting his new crypter, [redacted] lol So i checked his site, I noticed he closed [redacted] project, and he is selling the new one -- [redacted] And on his site , he wrote, old client who bought [redacted] 3 months can update to new [redacted] and with 1 month update support time . I found him on msn, he finally replied me, he said he can't update to [redacted] for me , becасue it has past 3 month, I told him , i kept trying to contact him , but he never reply me . And he said its all my fault becасue i don't check his post in opensc. lol .

He never replied me in the 3 month, so what is the difference to check opensc with his post or not ?? lol . That is the way of how this shit treat with his client . it happend a few month ago , but i decided to post it here , to make sure more people can see it , and do not buy anything from him , if you don't want to be treated like this .

plz check the screen shorts here , this is the chatting logs on msn, im sure you will like it :

[Large redacted area for chat logs]

Last edited by parkingcash; 06-05-2012 at 03:33.

Figure 11—A customer of LUCKY, who goes by the alias "parkingcash" complains how he purchased FlyCrypter in July 2011 and LUCKY promised three months of support with the purchase. However, LUCKY did not provide the support and did not respond to parkingcash's messages for three months.

Parkingcash was not the only threat actor to complain about LUCKY. On February 28, 2012, a hacker going by the alias “iskapo” complained to fellow hacker, “BlueCY,” that LUCKY not only ripped him off for \$100, but he also dodged all his messages. Iskapo wanted everyone to know that LUCKY was a Ripper. (See Figure 12).

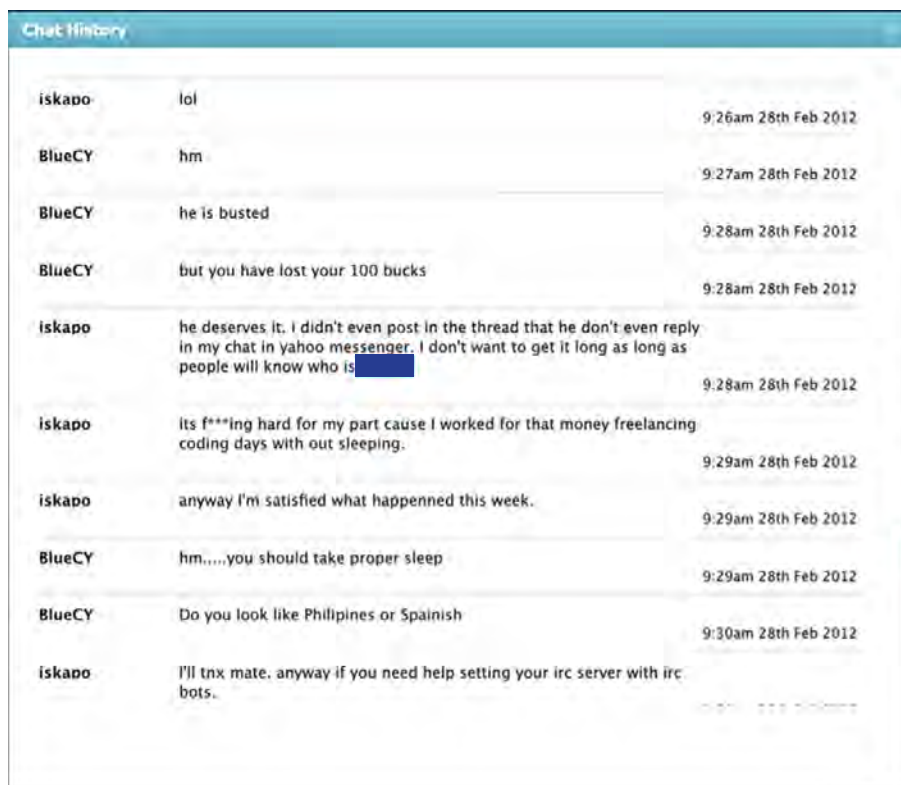


Figure 12—LUCKY’s customer iskapo complains to fellow hacker BlueCy that LUCKY took his \$100, and LUCKY wouldn’t even respond to his messages.

TRU finds other posts where threat actors are complaining about LUCKY, and they speculate that LUCKY doesn’t have time for his clients because “he’s such a party boy,” and he “is always in the bars and clubs.” (See Figure 13). By 2012, LUCKY would be 19 years old and could legally go to bars and clubs.

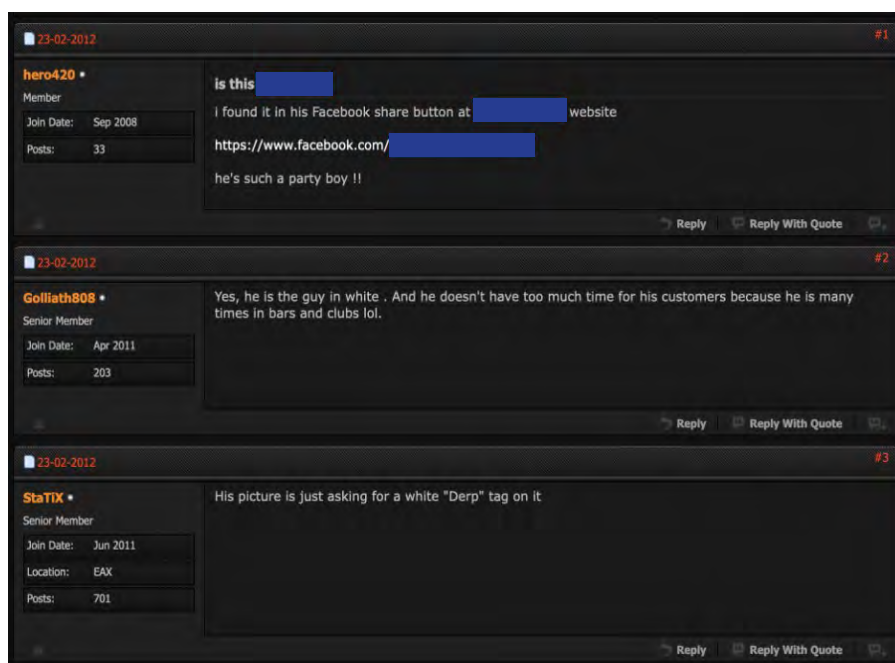


Figure 13—Underground forum members speculate that LUCKY is too busy hanging out at bars and clubs to spend time taking care of the customers.

Unfortunately, LUCKY's reputation as a "Ripper" continues to grow, as evident by a post dated March 5, 2012, by yet another disgruntled customer going by the alias: "zIFuLLiLeTe." He calls LUCKY "SCAMMER of the Year," and he also tries to warn potential buyers to stay away from buying any tools from LUCKY. "Everybody before buy this sh__ crypter read this..." "You don't even care about your customers until your sh__t got cracked...i see you only like \$\$\$." Interestingly, LUCKY's former disgruntled customer, iskapo, also chimes into zIFuLLiLeTe's chat about LUCKY (See Figure 14).

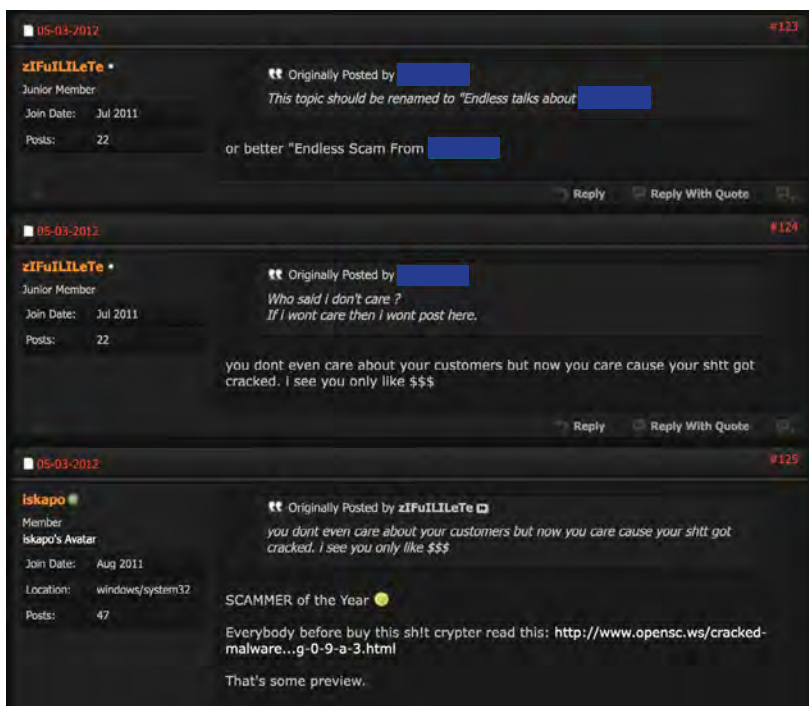


Figure 14—Another disgruntled customer of LUCKY posts that LUCKY is the “Scammer of the Year” and warns everyone to read about his crypter before buying it.

Trouble at work and at home

By the time April 2012 rolls around, it is evident that 19-year-old LUCKY has established a bad reputation for himself, and from several other posts, it appears that LUCKY has other “big life problems” as he describes them. In one chat, TRU sees LUCKY tell a friend he is thinking about moving to Pakistan. He says: “I have three trusted friends here, and I will work for the Pakistan gov. I just need the papers, that’s all.” LUCKY goes on to say “Reason: big life problems...it’s a long story. Basically i need to go in any other country except Romania.” See Figure 15.

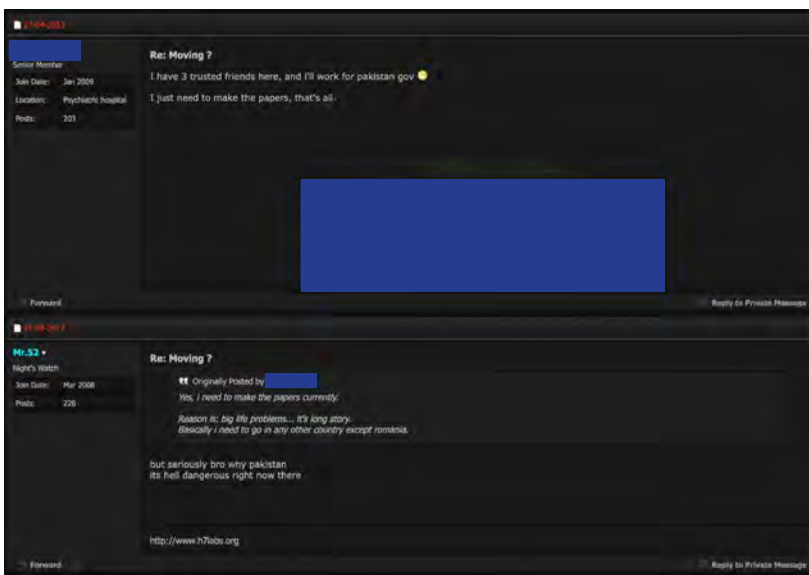


Figure 15—LUCKY says to a forum member he might go to Pakistan to work for the government because he has big life problems, and he needs to go in any other country except Romania.

TRU then finds LUCKY speaking to another threat actor, who goes by the alias: 1337 hax0r 3.- about his potential move to Pakistan. LUCKY appears to be fairly trusting of him because he discusses the possibility of going to work with the Pakistan government as a security specialist. In fact, he reveals to 1337 hax0r 3.- that he has one crypter customer who works for the Pakistan government, and he tells him that what he will be doing “will be hidden” (See Figure 16).

Some brief research into connections between LUCKY and Pakistan-sponsored cybercrime was explored by TRU, turning over some interesting coincidences (see more in the upcoming section titled: **Does LUCKY run off to Pakistan?**).



Figure 16—LUCKY discusses with a fellow threat actor his plans to work for the Pakistan government as a security specialist.

Whatever LUCKY's "big life problems" are it doesn't seem like he is able to go to his family for help, as evident from a May 2012 discussion between LUCKY and his confidante-- 1337 hax0r 3.-. LUCKY tells him that his father is dead and that he died in a car accident. He further confides in 1337 hax0r 3.- saying "my mother doesn't care about me...that is how she is. I've two little sisters and since that he forgot about me." LUCKY clearly feels isolated from his family, especially since his Father died (See Figure 17).

| Chat History | | |
|----------------|-----------------------------------|----------------------|
| | nope | 2:37pm 21st May 2012 |
| | my father is dead | 2:37pm 21st May 2012 |
| 1337 hax0r 3.- | cause? | 2:38pm 21st May 2012 |
| | my mother doesn't cares about me | 2:38pm 21st May 2012 |
| | cause nothing | 2:38pm 21st May 2012 |
| | this is how she is | 2:38pm 21st May 2012 |
| | i've two little sisters | 2:38pm 21st May 2012 |
| | and since that he forgot about me | 2:38pm 21st May 2012 |
| 1337 hax0r 3.- | no i mean cause of death | 2:38pm 21st May 2012 |
| | car accident | 2:38pm 21st May 2012 |
| 1337 hax0r 3.- | omfg | 2:40pm 21st May 2012 |

Figure 17—LUCKY confides in fellow threat actor 1337 hax0r 3.- that his father died in a car accident and that is Mother doesn't care about him, not since his two younger sisters came along.

Because TRU was able to uncover LUCKY's real name, the date and location of his birth, and that he lives in Bucharest, Romania, TRU was able to confirm that LUCKY does indeed have two younger sisters and a Mother living in Romania.

On December 28, 2012, there is a post on the Exploit.in forum in which LUCKY claims to have discovered and is sharing (for free) a NASA SQL server (See Figure 18). **Note:** One will see in the Exploit.in post, that there is a mark directly through the name LUCKY and underneath is the word RIPPER. This is significant because if the administrator of a forum gets repeated complaints about a forum member cheating and scamming his/her clients, then they will take the user's profile (in this case LUCKY) and tag them as a RIPPER. In the Exploit.in forum, the user profiles are always displayed to the left of every post and once an Exploit.in forum user gets tagged as a RIPPER, no matter how old the post is, their user profile will always show them as a RIPPER. Although LUCKY did not get tagged as a RIPPER on Exploit.in until 2014, all his previous posts display the RIPPER tag.

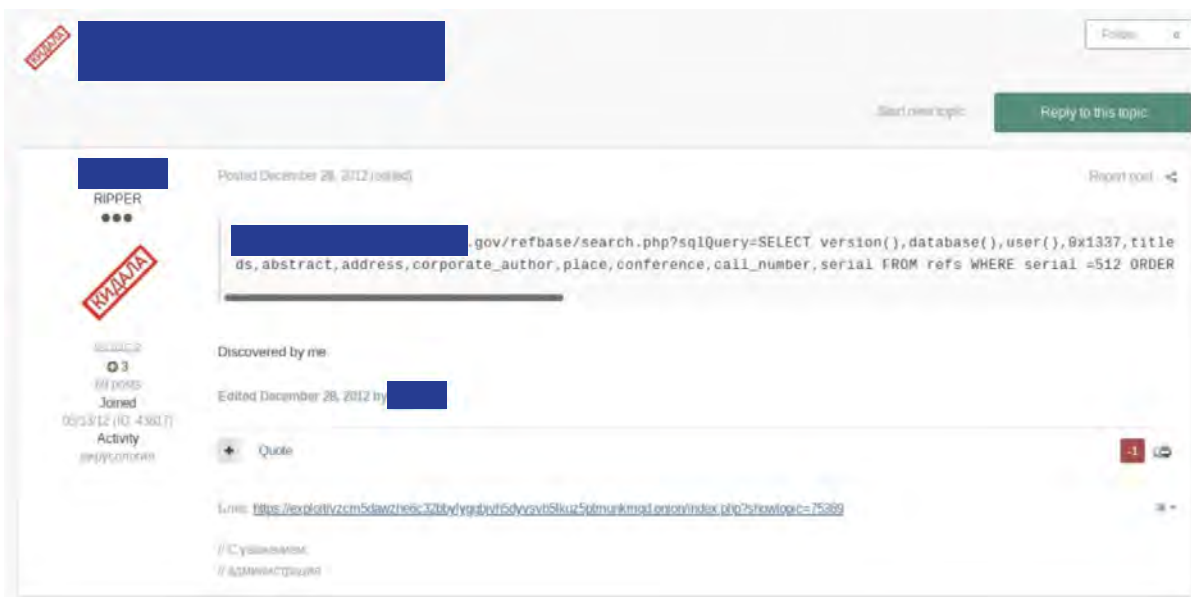


Figure 18—LUCKY shares an exposed SQL server owned by NASA on the Exploit.in forum.

Does LUCKY run off to Pakistan?

After seeing posts from LUCKY, where he seems to speak seriously about leaving for Pakistan, TRU wonders if he did go work for the government or for himself, developing and selling malware. It certainly seems plausible since he has 1) racked up a host of disgruntled customers, who are spreading the word on the underground that he is a Scammer/a RIPPER, 2) he appears to have gotten himself into some real trouble, so much so that he is contemplating leaving his home country, and 3) lastly, he believes that the only parent he has left, his Mother, doesn't care about him.

If LUCKY did go to Pakistan, there is an interesting coincidence. There is an Advanced Persistent Threat (APT) group called SideCopy. According to [news reports](#) they have been behind a number of attacks targeting the Indian defense forces and military personnel. They were first observed by security researchers in 2019 and are believed to originate out of Pakistan.

Security researchers contend that there is a tie between the SideCopy APT group and the APT group called [Transparent Tribe](#), who were first observed in 2013. Transparent Tribe is also known for launching cyberattacks against India's government and military, and as of late, has turned its attention to Afghanistan. Transparent Tribe is also suspected of being out of Pakistan.

Coincidentally, SideCopy's 2019 campaign features some similar tactics that LUCKY was using during the same time frame in what is now called his VenomLNK malware, an initial access vector of LUCKY's current more_eggs backdoor (the main component of LUCKY's Golden Chickens malware suite). The similarities in tactics include the use of 1) a malicious LNK file, 2) a Decoy Document, and 3) copying trusted windows binaries out of the system32 folder and into a user folder where the malware can abuse them (See Figure19). TRU finds it interesting that there are similar tactics, used by an APT group believed to be out of Pakistan, and malware that LUCKY has developed.

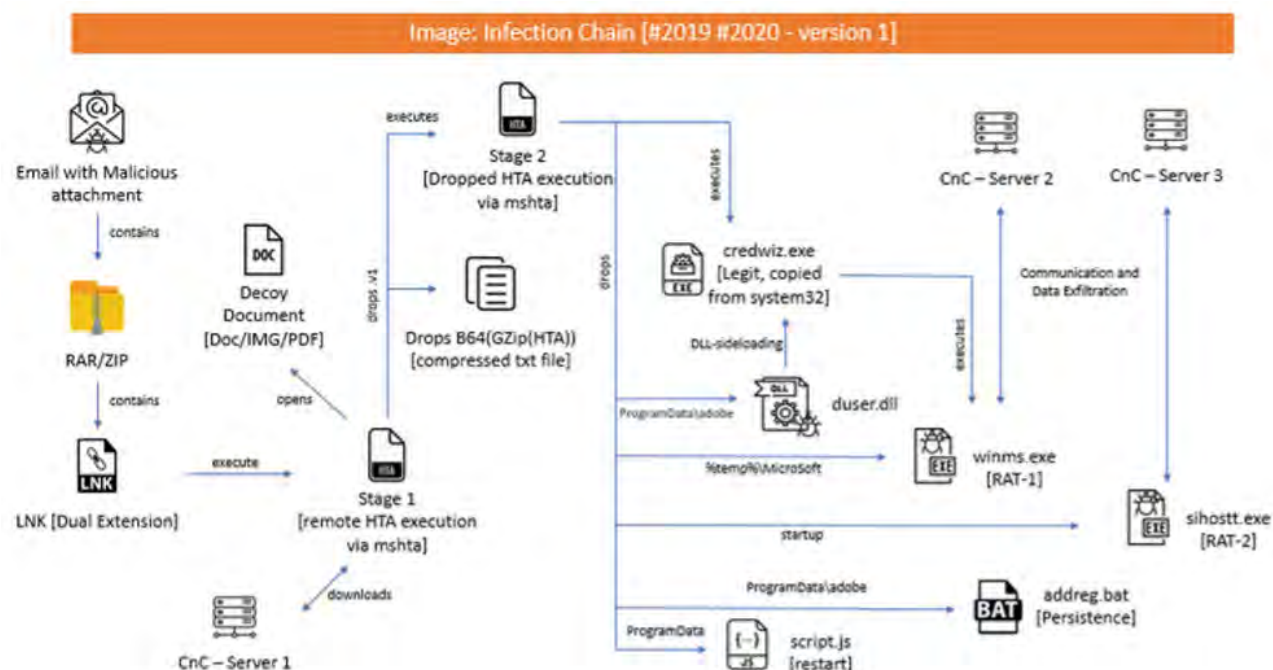


Figure 19—An infection chain used by SideCopy APT bears some high-level similarity to earlier versions of VenomLNK.

LUCKY/B3st/BEST emerges on the hacker scene under new aliases

As briefly touched upon at the beginning of this report, on October 4, 2013, TRU sees a post from the account badbullz on the Lampeduza forum, where a Canadian bank issued credit card is being advertised. Initially, TRU believed that it was simply "Chuck from Montreal" peddling a credit card, after all he is based in Montreal. Plus, TRU already established in part 1 of the report that he likes to deal in stolen credit cards. However, upon further inspection, TRU sees that the contact information is different from any they had ever seen "Chuck from Montreal" use for his badbullz accounts. The contact information was a jabber account TRU had never seen used by badbullz.

At that moment, a light bulb went off. TRU knew there was a second threat actor running the badbullz accounts, they just didn't have any leads as to who that second threat actor might be. When they discover this new jabber account, they think "this a small thread, but it is one we have to pull." (See Figure 20).

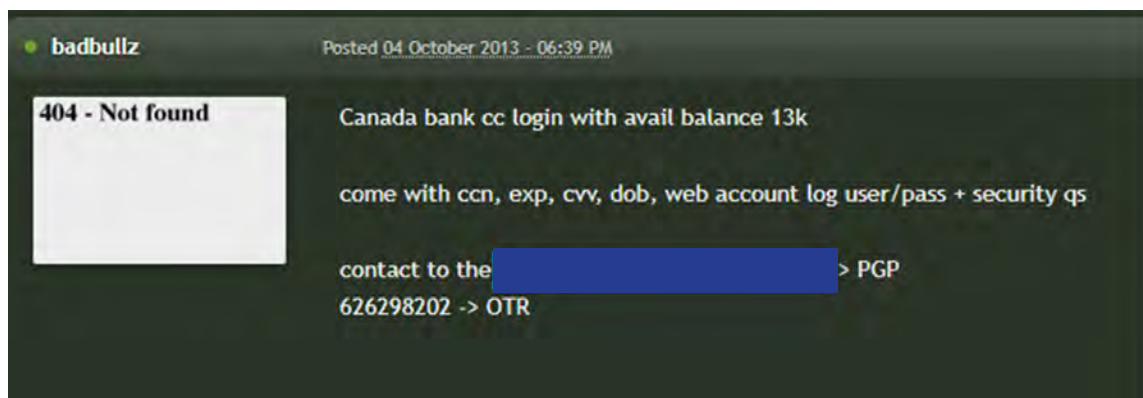


Figure 20—TRU sees for the first time, where the badbulliz account, uses a jabber account they had never seen before: as their contact information.

From that point forward, TRU dug into every forum database they could get their hands on, whether they were defunct or still operating. The amount of data that TRU culled through looking for this jabber ID equaled terabytes of data. After a couple of days — they found another instance of the jabber ID. They found a chat on the popular Russian forum, Verified, where a threat actor using the account name “LUCKY” was peddling Canadian traffic and his contact information just so happen to be the same as the jabber ID (See Figure 21).



Figure 21—LUCKY selling access to hijacked computers located in Canada and asking interested parties to contact him at his jabber address.

From there TRU dug in, and the hunt was on for LUCKY and everything TRU could find out about him: what role he plays in the Golden Chickens MaaS, his real name, his life in cybercrime, how he is connected to “Chuck from Montreal”, his education, where he lives, etc.

“Chuck from Montreal” meets LUCKY

TRU believes that at some point, between the latter part of 2012 and October 2013, LUCKY met “Chuck from Montreal” on the underground, and LUCKY brokered a deal with Chuck. The agreement was that Chuck would allow LUCKY, along with himself, to post under his account “badbullz” and “badbullzvenom” on a number of forums.

This was very clever on LUCKY’s part, because by 2013 he was labeled a RIPPER and a SCAMMER on multiple forums. LUCKY needed an account that had a pre-established reputation. He needed one that would allow him to continue to do business on the forums, where he was no longer welcome, and “badbullz” and “badbullzvenom” fit the bill.

It is not hard to imagine “Chuck from Montreal” and LUCKY crossing paths in the hacker underground around 2013. As TRU revealed in part I of the Venom Spider report, Chuck was highly interested in Canadian-based credit cards and bank account credentials for the top Canadian banks: TD, CIBC, Scotiabank, and BMO. TRU also detailed in part 1 that Chuck was a member of two underground carding forums: Carder.pro and Carder.su. Although they are currently defunct, they were two of the most popular carding forums on the underground. Carding forums are where buyers and sellers of stolen credit cards and debit cards, from around the world, connect with one another in order to transact business.

Meanwhile, from the previous examples in Figure 21 and 22, it is apparent that LUCKY is able to obtain account credentials for credit cards issued from Canadian banks, and he has access to computers located in Canada for sale. Therefore, it is not surprising that “Chuck from Montreal” and LUCKY met one another. **Note:** In 2013, although LUCKY had already begun posting under the badbullz account in some forums, there were some examples in 2014 where he continued to post under the LUCKY account. An example of this can be seen in Figure 22. TRU believes these are forums where LUCKY has not been blackballed, yet.

The LUCKY accounts go inactive, while the badbullz and badbullzvenom accounts take on a new life

For the threat actor behind the LUCKY accounts, 2015 was a milestone in several respects. This is the year he unveiled his new tool. TRU is calling it MULTIPLIER. TRU considers MULTIPLIER the beginning of what would later become the infamous Golden Chickens MaaS. MULTIPLIER is a kit for building macros. Macros are snippets of code that can be embedded into a Microsoft document and can execute malware. In the case of MULTIPLIER, the kit can be used to build macros for any type of Microsoft Office document: word, excel, powerpoint, etc. MULTIPLIER is thought by TRU to be the predecessor to the tool VenomKit.

This is also the year where one of LUCKY’s tools is not released under any LUCKY accounts, it is released under a badbullzvenom account. TRU believes, with the release of MULTIPLIER, the threat actor behind the LUCKY account ceases posting under this account or those that are similar, from this point forward. He only posts under the accounts of badbullzvenom and badbullz. By using the badbullzvenom and badbullz accounts, and unbeknownst to forum members, he is essentially starting with a clean slate, and he can continue to build his credibility under the account aliases: badbullz and badbullzvenom.

While still selling his MULTIPLIER kit in 2015 and 2016, TRU observes badbullzvenom (aka: LUCKY) continuing to show interest in crypters and banking trojans. TRU also sees badbullzvenom (aka: LUCKY) bantering back and forth with other threat actors. Although he does give several fellow hackers a “thumbs up” for some of their tools and malware, he continues making aggressive comments, showing that he has a short fuse and can get aggressive in his comments. One of these included a statement where he tells one member of Exploit.in “to kill themselves, and he offers to pay for the bullet.”

Badbullzvenom's (aka: LUCKY, B3st, best_LUCKY) malware continually improves and the top cybercrime gangs take notice

By 2017, badbullzvenom (aka: LUCKY) really began to hit his stride as a professional malware provider. He debuts his newest tool, and he calls it "Word 1-day doc builder," known today as VenomKit. Word 1-day doc builder is a kit for building malicious Microsoft Word documents. Badbullzvenom (aka: LUCKY) accumulates customers quickly for his new malware and continues making improvements. He adds new features and eventually removes PowerShell from the kit to reduce detection by anti-malware and antivirus products. He also adds .dll support for the payloads and a JS Downloader (this is likely the predecessor to the TerraLoader component of the Golden Chickens malware suite) to the Word 1-day doc builder kit. It is offered for sale as an add-on.

Badbullzvenom (aka: LUCKY) continued developing additional malware to work alongside his Word 1-day doc builder until he finally established a stealthy, highly functional, all-in-one suite of malware. It consists of various components that threat actors can select for their objectives. It is currently known as the Golden Chickens MaaS.

All of badbullzvenom's development work paid off because according to security reports, in 2017 his malware caught the attention of a customer that wasn't just any run-of-the-mill hacker. It was a threat group considered to be one of the most infamous financial crime groups in existence. It is Russia-based **Cobalt Group**. Cobalt Group is said to have caused the financial industry over a billion dollars in cumulative losses. Their crime spree includes the targeting of 100 financial institutions in more than 40 countries worldwide, allowing the criminals to steal more than US\$11 million per heist.

Security experts assert that in 2017 the Cobalt Group used badbullzvenom's (aka: LUCKY) VenomKit to deploy Cobalt Strike in attacks on banks – and then they used it again in 2018. Cobalt Strike is a common tool used by threat actors to gain a foothold in an organization's IT network and then further expand their access.

The Cobalt Group was not the only crime syndicate to take notice of badbullzvenom's (aka: LUCKY) Golden Chickens malware suite. It also attracted the likes of top financial crime group, **FIN6**, who is also based out of Russia. They are known as one of the most notorious hacking gangs in the world of cybercrime. They dominated news headlines in 2018 when they were cited as being the cyber group who broke into the online payment systems of **British Airways**, **Ticketmaster UK** and top electronic retailer, **Newegg**, stealing credit and debit card data from millions of customers. Conservatively, security firm Trellix estimated that in one of their campaigns FIN6 stole 20 million payment cards worth US\$400 million.

It was in 2019 that **FIN6** was first observed using the Golden Chickens MaaS (previously referred to as more_eggs) in an attack campaign involving "employment lures." However, this would certainly not be the last cyber campaign involving Golden Chickens and "employment lures."

In 2019, security researchers also saw the PureLocker ransomware plugin emerge as a component of the Golden Chickens offering. It was **being used in targeted attacks** against workstations and production servers running Windows and Linux. PureLocker takes its name from the language used to author it: PureBasic. Interestingly, LUCKY has demonstrated knowledge of, and a preference for PureBasic in online discussions

The Golden Chickens MaaS is alive and well

In April 2021, TRU detected a significant Golden Chickens campaign, and almost exactly one year later, they uncovered a second round of attacks involving the Golden Chickens malware. Barely two months after that, in July 2022, TRU spotted a third campaign.

Interestingly, all three Golden Chickens campaigns involved employment lures. Either the campaigns targeted corporate employees on [LinkedIn](#), using fake job offers, laden with malware, or they targeted **corporate hiring managers** with fake resumes of job applicants, laden with malware. The campaign that kicked off in November 2022 has continued with TRU detecting and shutting down the most recent Golden Chickens attack in January 2023. In this campaign, TRU saw evidence that the malware is being used to go after e-Commerce companies, in addition to service companies—and all of them have online payment systems. Ironically, in FIN6's 2019 Golden Chickens campaign, they also used employment lures and went after e-Commerce companies, being that it is a favorite target of the financial crime group, having had so much success in compromising British Airways, Newegg, Ticketmaster and countless others.

Note: Interestingly, during the first week of May 2023, TRU found that two identical samples of the Golden Chickens VenomLNK component were uploaded to VirusTotal. One sample was uploaded from the Ukraine, and one was uploaded from the U.S. This might indicate an attempt by threat actors to launch a new Golden Chickens attack campaign or it might indicate testing by the threat actors.

The Golden Rule of Golden Chickens: “Mass spamming is not allowed. You spam, You banned. Simple.”

One might think that three malware campaigns in twenty-one months isn't significant. However, the infrequency and the specific targeting of the Golden Chickens campaigns is very intentional by the threat actors operating the attacks and the creator of the malware, badbullzvenom (aka: LUCKY).

In fact, in one post from badbullzvenom (aka: LUCKY) in Exploit.in, he bans a customer called Black Angus because he found a sample of his Golden Chickens malware in VirusTotal. Badbullzvenom tells Black Angus in no uncertain terms “Mass spam is not allowed. If hash is found in virustotal in less than four days, then you get banned (no rebuilds possible).” He continues with: “You broke the terms > You are banned. simple.” He ends with “my softwares aren't for you, you don't do targeted attacks.” See Figure 22.

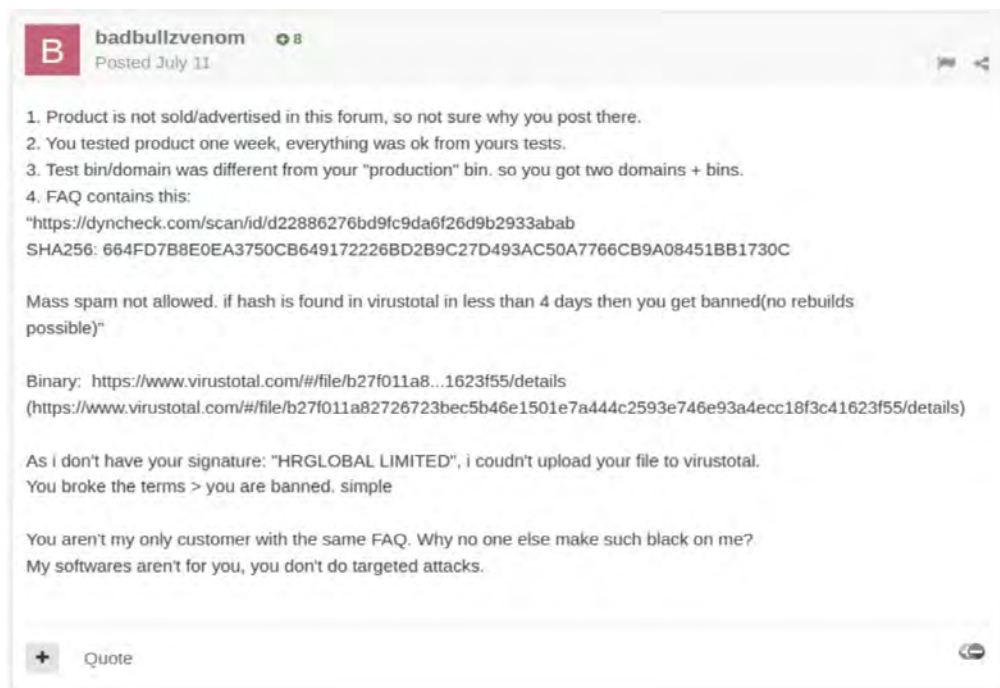


Figure 22—Exploit.in reply to dispute thread. badbullzvenom drops BlackAngus as a customer for breaking his rules and shuts down his access.

Following the Gravatar link and Discovering the man behind LUCKY (aka: Jack, badbullz, badbullzvenom) and the creator of Golden Chickens?

So, who is the real man behind the LUCKY accounts, who self-identifies as “Jack” and who has been posting under the badbullz and badbullzvenom accounts since 2013? Who is the real creator of Golden Chickens and how did TRU discover his identity?

Once TRU knew that the LUCKY identity was operating the badbullz and badbullzvenom accounts at times, they started searching for any other related forum or social media accounts using that name or emails connected to that alias. TRU discovered a Gravatar account belonging to one of the email addresses LUCKY had used to register for several forums. Gravatar is a web service that lets users upload an online avatar and will associate the avatar with their email address.

Although Gravatar obfuscates the email address of the account owner using MD5 hashes, it is often trivial to link a Gravatar account to the owner’s email address simply by brute-force, generating the corresponding hashes of billions of email addresses sourced from leaked email address lists circulating on the underground. Conversely, when searching Open-Source Intelligence (OSINT) sources for an email address, it is recommended to also search for the MD5 hash of the email on Gravatar’s servers, because in many cases (including this one), the returned metadata includes the full name of the account owner.

Of course, this account could have been registered with a completely fake name, so it’s always important to get independent confirmation of any such links. By searching for the term “LUCKY” in combination with the Gravatar-revealed “name,” TRU located a comment dated 2013 from an anonymous tipster on a security blog, asserting that the name revealed by Gravatar was the real name of LUCKY.

From here, TRU was able to locate the social media accounts of a Romanian citizen with the same name, whose personal details matched those revealed by or leaked about LUCKY, such as his location (Bucharest), hometown (Mizil) and living family members (mother and two younger sisters). Although “Jack” (aka: LUCKY, badbullzvenom, badbullz) is quiet on social media, these accounts and their social networks allowed TRU to build a picture of “Jack’s” personal life, his family, his lifestyle and his travel. TRU was also able to find that “Jack” is married, and he is listed as the owner of a vegetable and fruit import and export business. Further mining the social media accounts, TRU was able to locate an upscale area of Bucharest where they believe “Jack” and his wife reside.

Readers, meet "Jack", the real creator of the Golden Chickens MaaS

"Jack" (LUCKY, badbullzvenom, badbullz) enjoys the good life

From the various pictures on "Jack's" (LUCKY, badbullzvenom, badbullz) wife's social media accounts, it appears that "Jack" really started to find success in 2019. There are pictures of "Jack" and his wife in 2019 visiting many of the top cities in the world, including London, Paris, and Milan.

It also appears from the photos that they both enjoy designer clothing. In this photo, LUCKY is sporting a designer t-shirt from Dsquared2 which runs between USD \$200 and \$250 (See Figure 24). In a second photo, LUCKY and his wife toast champagne, with London in the background. She is wearing what appears to be an authentic Valentino purse, which can retail for anywhere between USD \$3,000 and \$5,000 (See Figure 25).

The last photo is of LUCKY and his wife, perhaps on their honeymoon, wearing matching robes (See Figure 26).



Figure 23—Jack, the creator of the Golden Chickens MaaS, at a coffee shop outside the Manufaktura Mega Mall in Bucharest.



Figure 24—LUCKY with his wife sporting a DSQUARED2 designer t-shirt which costs between USD \$200 and \$250.

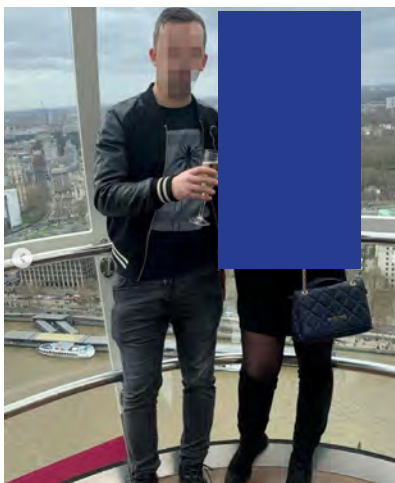


Figure 25—LUCKY and his wife toast champagne, with London in the background, with her wearing what appears to be an authentic Valentino purse, which can retail for anywhere between USD \$3,000 and \$5,000.



Figure 26—LUCKY and his wife, perhaps on the honeymoon, wearing matching robes.

A \$200,000 bounty issued for badbullzvenom on July 18, 2022

Although badbullzvenom (LUCKY, B3st, best_LUCKY) appears to have found success, his short temper and habit of “Scamming/Ripping” off his customers seemed to have reemerged and caught up with him.

On July 18, 2022, a threat actor going by “babay” went on Exploit.in and accused badbullzvenom of stealing \$1 million from him. Consequently, babay issued a \$200,000 bounty for any information leading to badbullzvenom’s real identity. (See Figure27).

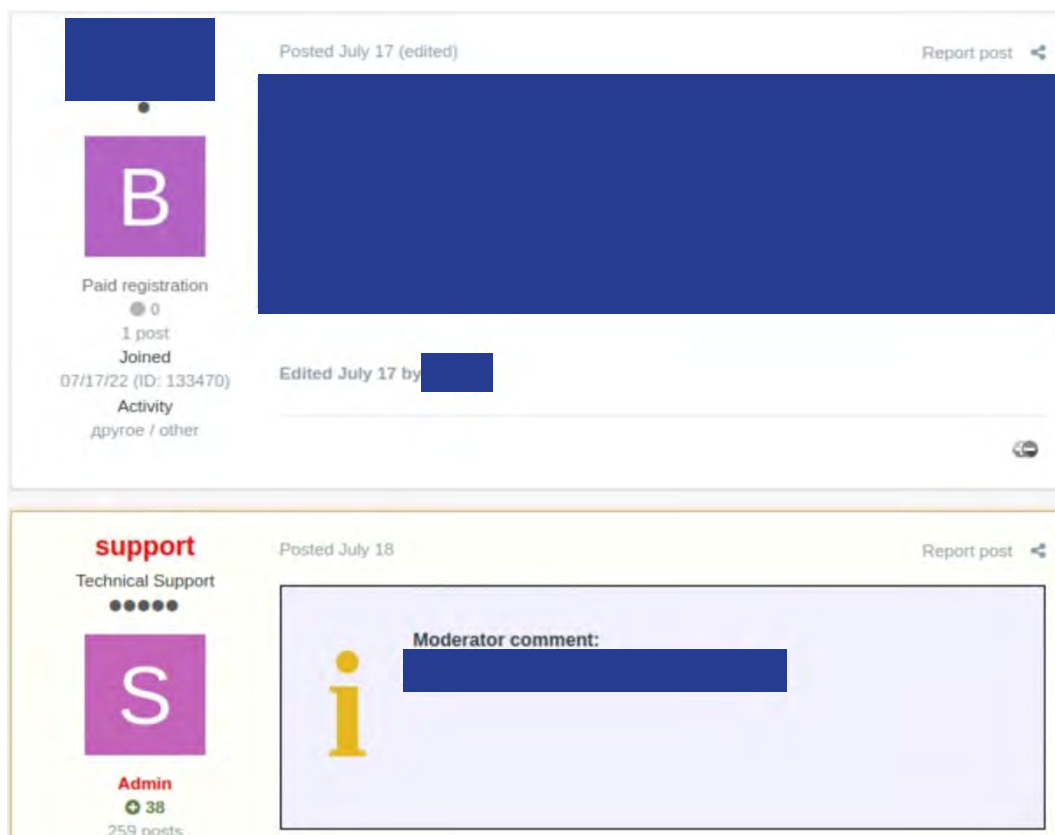


Figure 27—A threat actor on Exploit.in accuses badbullzvenom of stealing \$1 million from him and offers a \$200,000 bounty for any information leading to his real identity

The translation of the complaint made by babay about badbullzvenom:

The total cost of the complaint \$1,000,000.

The person scammed me, didn't complete his job, talk total nonsense, I can't contact him and he refuses to return the money back. The situation is private, I sent the logs to the admin.

For the information that can lead to his deanonymization I will pay \$200,000 through the guarantor."

LUCKY's fatal mistake

The threat actor who went by the alias LUCKY and who also shares the badbullz and badbullzvenom accounts with the Montreal-based cybercriminal "Chuck," made his fatal mistake when he used the jabber account. It was this jabber ID which led TRU to discover the LUCKY account and subsequently the real threat actor behind LUCKY and partner to "Chuck from Montreal".

"We suppose that, like a lot of new hackers just starting out, LUCKY never imagined that in the future, security researchers would gain access to countless leaked databases, enabling them to build a comprehensive history of a threat actor's public (and sometimes private) messages, online aliases, ICQ and Jabber ID's, going back over 15 years. This turned out to be a fatal oversight for his operational security," said Joe Stewart, Principal Security Researcher, TRU.

The significance of discovering the identity of the author and operator of the Golden Chickens MaaS

- I. **Better Understanding of the Technical, Tactical, and Strategic Operations of the Golden Chickens Service Offering**—With this investigation, TRU was able to build an accurate picture of the Golden Chickens malware author's Techniques, Tactics and Procedures (TTPs). TRU uncovered specific details, from the author's public and sometimes private conversations, showing his progression from a young teenager interested in hacking tools to a professional malware provider.

Throughout the course of this investigation, TRU was able to develop detections, track infrastructure, and gain context around the technical, tactical, and strategic operations of the Golden Chickens service offering. This alone makes attribution analysis valuable – even when it doesn't lead to the identification of cybercriminals. It is often what you learn along the way that can have the most impact in the field. Observing firsthand the technical, social, and transactional nature of cybercrime gives rare insights into the motivations and challenges threat actors come across and help to explain observations in the field that otherwise can leave analysts scratching their head. These observations alone can help security defenders position themselves against attacks.

- II. **Disrupting the Cybercriminals' Supply Chain**—When attribution analysis is conducted and it leads to identification, as in the case of Venom Spider, the impact to society becomes even more significant. Hackers are real people with real problems – and a lifestyle of cybercrime is fraught with paranoia and anxiety, as is often conveyed in [interviews](#) with threat actors. A published attribution report can therefore act as a damping force on cybercrime activity, reducing business opportunities and forcing threat actors to be more selective in future operations or quit the game all together. When the threat actor is a Malware-as-a-Service provider like Venom Spider, and suddenly he is no longer able to provide his malware service this disrupts his customers' business forcing them to find another malware source.


- III. **Sociopsychology of Cybercrime**—Investigations such as these, provide insight into the social psychology of cybercrime. Threat actors are, inevitably, human. They have human problems, and they require human connection. This can have numerous repercussions for them as they make their way through the underground markets in an attempt to establish a reputation. The death of a father can lead to a new version of malware, legal troubles can lead to a shift in business associates, and online disagreements and fights can expose links between threat actors, their business associates, and the malware they develop or use (e.g., badbullzvenom). TRU contends the more security professionals know about their enemy, the better prepared they will be to defend their organization against their enemy, taking inspiration from the saying: "You Must Know Your Enemy, To Defeat Your Enemy."

Conclusion

TRU assesses with high confidence, given the evidence detailed in this report, that the threat actor who self-identifies as “Jack” is the key operator and creator of the Golden Chickens MaaS. TRU expects cyberattacks, using the Golden Chickens MaaS, to continue in the first half of 2023. TRU is continuing to investigate the Golden Chickens operation and any other parties that may be involved.

It is TRU’s recommendation that organizations take the following steps to protect against the Golden Chickens malware suite:

1. Employ exhaustive endpoint monitoring for LOLBINs, aka **Trusted Windows Binary abuse**. LOLBINs of interest include cmd.exe, wscript.exe, wmic.exe, cmstp.exe, msxsl.exe, powershell.exe, and ie4uinit.exe. Ensure endpoint products have rules in place to detect suspicious usage of these Windows processes.
2. Ensure employees are aware of common phishing tactics:
 - a. Be suspicious of attachments from people you don’t know – additional care is required in cases where you must accept documents from the public (such as with employee hiring process)
 - b. Inspect attachment file types by right clicking the file and selecting properties
 - c. Documents should never come as LNK, ISO, or VBS files
 - d. Often, these malicious files will be enclosed in a .zip file to bypass email filters
3. Have an easy process in place for reporting phishing and suspicious behavior
 - a. Leadership is responsible for ensuring a positive and convenient path is in place for reporting suspicious behavior
 - b. Develop a collaborative culture of cyber resiliency where employees are comfortable to bring forward questions, and even mistakes when it comes to email behavior and downloads. Punishing employees for falling for phishing scams will reduce the chances that they – and other employees – report them in the future.
4. Engage **Managed Detection and Response** services for 24/7 Security Monitoring, Threat Hunting and Threat Containment expertise. The speed with which you can detect and contain a threat actor before they achieve their objectives is imperative in preventing business disruption.

If you’re experiencing a security incident or breach, contact us  1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization’s cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world’s most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire’s award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit www.esentire.com and follow @eSentire.